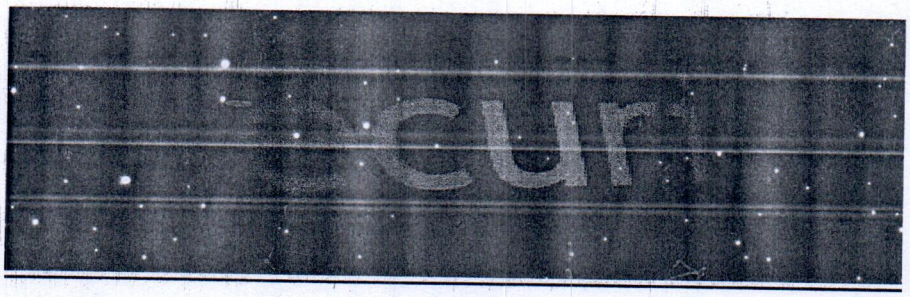
Mody University of Science and Technology
College of Engineering & Technology
Lakshmangarh – 332311, Distt. Sikar (Rajasthan)
Phones: (01573) 225001 to 225012 (12 lines) Fax: (01573) 225042

Research Proposal

on

Security in Wireless Sensor Network



Under the Supervision of:

Prof. M.K. Jha
Associate Dean

Submitted by:

Ms.Uma Meena
E.No. 070761

Introduction of the topic:

➢ Wireless Sensor Networks: [1]

- A network consisting of hundreds or thousands of wireless sensor nodes.
- Collect information from their surrounding environment and send to remote control center.
- Each node comprises of:
- Transducer: A transducer is an electronic device that converts energy from one form to another. They can sense pressure, temperature, sound, vibration, pollutants, chemical sensor (measure chemical composition of soil).
- Processor (Processing capability)
- Memory
- RF transceiver
- Power source (Battery, solar)

➢ Security Needs in WSN: [2]

- The broadcast nature of WSN can be easily eavesdropping by attackers, hence symmetric key cryptography is used.
- To avoid the capturing or reprogramming of secret data by attackers.
- To save the entire WSN from radio jamming.

➢ Elliptic Curve Cryptography: [3]

- ECC was introduced by Victor Miller and Neal Koblitz in 1985.
- ECC as an alternative mechanism for implementing public-key cryptography.
- The good thing about Elliptic Curve Cryptography (ECC) is that it can be faster than RSA and uses smaller keys, but still provides the same level of security.
- ECC requires significantly smaller key size with same level of security.

- An elliptic curve is a plane curve defined by an equation of the form:

$$y^2 = x^3 + ax + b$$

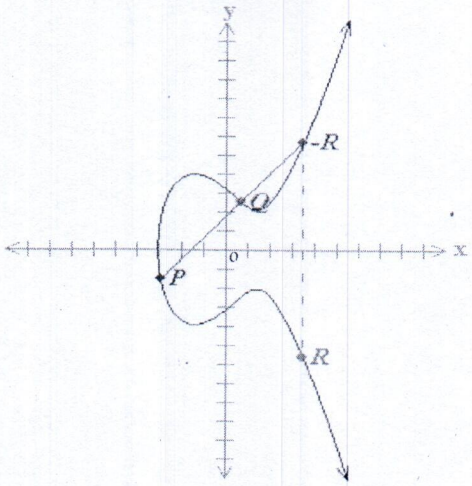


Figure1: Point Addition

- If P and Q are two points on E, we can define :

$$R = P + Q$$

- Like this we can perform various operations on elliptic curve such as subtraction, multiplication, and inverse.

- **Why use ECC?**

✓ Smaller key size

✓ Faster than RSA

✓ Good for handhelds and cell phones.

❖ **Key Generation:**

- In Key generation, we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

- **Steps are as follow:**

1. Choose a large prime *p.*

2. Choose an elliptic curve *E* defined over *GF (p).*
3. Choose a point *G* on *E* with prime order *n.*
4. x ε_R [1, n-1].
5. Calculate public key *Y* as *Y = xG*
6. Find a homomorphic encoding function *Φ ()* that maps a message *m* to a point *M* on *E.*

❖ **Encryption:**

- **Steps are as follow:**

1. Calculate *M = Φ (m).*
2. *k* ε_R *[1, n-1].*
3. Encrypt the pair *(C1, C2)* as *M = (KG, KY+M)*

❖ **Decryption:**

- **Steps are as follow:**

1. Decrypt the pair *(C1, C2)* as *M = -xC1 + C2.*
2. $m = \Phi^{-1}(M)$.

Problem definition:

- Most of the WSN's have the limitations of high computational and communication overhead in addition to lack of scalability to node compromise attacks. However, polynomial-based scheme and its extensions have the weakness of built-in threshold that is determined by degree of polynomial. This scheme was recently introduced. Also we have studied the comparison of the results of proposed scheme and polynomial based approach with the help of ns-2 tool.
- Now we are doing this comparison of proposed protocol and polynomial-based approach with the help of Matlab.

Expected output (results):

- The security of the data is increased by implementing the proposed scheme so that it overcomes all the disadvantages that were there in polynomial-based approach and symmetric key cryptography and also provide confidentiality to make data more secure as well as confidante.

Review of recent related works:

➢ **"Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks"** [4]

- **Abstract:** Message authentication is one of the most effective ways to thwart unauthorized and corrupted messages from being forwarded in wireless sensor networks (WSNs). For this reason, authors proposed two message authentication schemes are as follows:
- Symmetric-key cryptosystems / Shared-key cryptosystems.
- Public-key cryptosystems / Asymmetric -key Cryptosystems.

- But the symmetric-key based approach have some limitations such of high computational and communication overhead, requires complex key management, lacks of scalability, and is not resilient to large numbers of node compromise attacks. To address these issues, a polynomial-based scheme was recently introduced. However, this scheme also has the weakness of a threshold i.e. determined by the degree of the polynomial. When the number of messages transmitted is below the threshold, the scheme enables the intermediate node to verify the authenticity of the message through polynomial evaluation. However when the number of messages transmitted is larger than this threshold, the polynomial can be fully recovered and the system is completely broken.
- To overcome threshold problem, authors proposed **Source Anonymous Message Authentication (SAMA) scheme** is based on the optimal Modified ElGamal

Signature (MES) scheme on elliptic curves that provides hop-by-hop node authentication without threshold limitation.

- **We need to determine:**

✓ **Key size:**

- For bivariate polynomial-based scheme authors choose key size l and
- For proposed scheme, ECC should be 2l which is much shorter than the traditional public-key cryptosystem.

✓ **Degree of polynomial:**

- For the bivariate polynomial-based scheme, determine dx and dy, and
- For proposed scheme, determine n.
- In simulation, authors selected dx equal to dy, three values are as follow: 80, 100, and 150.

- **Experimental Results:** For implementation authors take two platforms: Mica2 platform, which is 8 MHz and Telosb platform, which is 4 MHz.

- **Conclusion:** Both theoretical and simulation results show that, proposed scheme is more efficient than the bivariate polynomial-based scheme in terms of computational overhead, energy consumption, delivery ratio, message delay, and memory consumption.

➢ **"Secure Data Discovery and Dissemination Based on Hash Tree For Wireless Sensor Networks "** [5]

- **Abstract:** In this paper authors proposed several approaches for data discovery and dissemination in WSN's that ensure the reliability and securities issues in a network.
- During data discovery and dissemination in WSN's, some security vulnerabilities are identifies such as:

✓ an adversary update a network with undesirable values,

- ✓ erase critical variables.
- To address these vulnerabilities, paper presents a new protocol named SeDrip, which provides secure data delivery.
- Several data discovery and dissemination protocols have been proposed such as Drip, DIP and DHV only address reliable data transmission but provide no security mechanism.

- **Effects of Security vulnerabilities in data discovery and dissemination:**
- ✓ an adversary can reboot the entire network with wrong data,
- ✓ can inject a fake data to the networker
- ✓ erase an important variable.

- **SeDrip based on the following assumptions:**
- ✓ The base station cannot be compromised and it trustworthy.
- ✓ The B.S. has unlimited computational power.

- **Description of SeDrip protocol :**
- SeDrip is based on ECC approaches as compare to public-key cryptography in terms of key size, computational efficiency and communication efficiency.
- Based on Merkle Hash Tree operation.
- SeDrip consists of three phases:
- ✓ System initialization
- ✓ Packet pre-processing
- ✓ Packet verification
- To improve SeDrip protocol we use Message specific Puzzle Approach.

- **Conclusion :**
- The SeDrip protocol allows efficient authentication of data with the help of Merkle tree algorithm. This protocol works in the limitation of memory, energy and computation, which shows that SeDrip is efficient and feasible in practice.

➢ "SDRP: A Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks" [6]

- **Abstract:** In this paper authors developed a secure and distributed reprogramming protocol named SDRP that is used to secure the reprogramming and to reduce storage requirements of each node.
- The reprogramming protocols are based on centralized or distributed reprogramming approaches.
- Distributed reprogramming approach is good than centralized reprogramming approach.
- SDRP is a first proposed protocol for distributed programming.
- Requirements for distributed reprogramming approach are as follow:

✓ Authenticity and integrity of code images
✓ Freshness
✓ Distributed
✓ User traceability
✓ Scalability

- Centralized reprogramming protocol consists of two kinds of participants, the base station and all sensor nodes.
- Distributed reprogramming protocol consists of three kinds of participants, the network owner, authorized network users and all sensor nodes.

- **Description of SDRP :**
- SDRP is based on ECC approaches as compare to public-key cryptography.
- SDRP consists of three phases:

✓ System initialization
✓ User preprocessing
✓ Sensor node verification

- **Conclusion and Future work :**
- SDRP is only one protocol, which is feasible in practice and that allows authorized users to reprogram sensor nodes in a distributed manner.
- And in future work, authors will study how to support confidentiality in distributed reprogramming i.e. providing high security to data in distributed network.

Research Plan (Include Time frame- literature review, data collection if any, how proposal will be tested, publications)

- **Literature review:**
- From January 2014 to December:

✓ Completed the course work.

✓ Literature review on wireless body area network.

- From January 2015 till date:

✓ Literature review on wireless sensor network security using elliptic curve cryptography.

- **How proposal will be tested:**

✓ Matlab

- **Publications:**

✓ Uma Meena and M.K.Jha, "An Efficiency Model for Authentication Approaches in WBAN", *9th INDIACom; IEEE 2nd International Conference on "Computing for Sustainable Global Development"*, ISBN 978-93-80544-15-1, pp.476 – 482, March 2015.

Benefits of Research: [4]

- The adversaries cannot modify the message content without being detected.
- The adversaries cannot inject fake message into the network without being detected.
- The adversaries cannot determine the message sender's ID.
- It is efficient in terms of both communicational and computational overhead.

References:

- [1] Dina S. Deif *and Yasser Gadallah,* "Classification of Wireless Sensor Networks Deployment Techniques", *IEEE COMMUNICATIONS SURVEYS & TUTORIALS,* VOL. 16, NO. 2, SECOND QUARTER 2014, pp.832-855.
- [2] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou, "Sensor Network Security: A Survey" , *IEEE COMMUNICATIONS SURVEYS & TUTORIALS,* VOL. 11, NO. 2, SECOND QUARTER 2009, pp.52-73
- [3] Hailiza Kamarulhaili, "Generating Elliptic Curves modulo *p for Cryptography* using *Mathematica software" , 2010 Seventh International Conference on Computer Graphics, Imaging and Visualization*,pp.92-96.
- [4] Daojing He, Chun Chen, Sammy Chan, Jiajun Bu, "SDRP: A Secure and Distruibted Reprogramming Protocol for Wireless Sensor Networks", *IEEE Trans on Industrial Electronics.* Vol. 59, no.11, pp.4155-4163, November 2012.
- [5] Daojing He, Sammy Chan, Shaohua Tang and Mohsen Guizani, "Secure Data Discovery and Dissemination based on Hash Tree for Wireless Sensor Networks", *IEEE Trans on wireless communications.* Vol. 12, no. 9, pp.4638-4646, September 2013.
- [6] Jian Li, Yun Li, Jian Ren, and Jie Wu, "Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks", *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS,* VOL. 25, NO. 5, MAY 2014.